CLAIMS

I Claim:

1. Authorisation method for an enrolled user of a limited access system presenting himself at a remote location to obtain access to said system, wherein the system having an authorisation centre and said remote location being provided with a remote terminal connected to the system, **characterised** by the steps of:

at the time of enrolling said user to said system

- assigning an identification code to said user and storing the assigned identification code at the authorisation centre;

- assigning a symbol set selection algorithm to said user and storing the assigned symbol set selection algorithm at the authorisation centre in association with the identification code of the user, wherein the symbol set selection algorithm being a list of instructions how a predetermined number of graphic symbols can be generated from a table of graphic symbols, wherein each graphic symbol is characterised by a predetermined number of dominant features and each dominant feature can take a number of values; and

at the time when said user presenting himself at the remote location for obtaining access

- displaying for said user on said remote terminal a table of a predetermined number of randomly chosen different graphic symbols so that the user can apply the assigned symbol set algorithm for generating a predetermined number of generated symbols;

- forwarding said generated symbols to said authorisation centre;

- forwarding said user identification code from the remote terminal to the authorisation centre;

- at the authorisation centre using the received identification code and reproducing said generated symbols by using the symbol selection algorithm associated with the identified user and comparing the locally reproduced response symbols with the ones received from the remote terminal, and providing access to said user only if the received and generated symbols being identical.

2. The authorisation method as claimed in claim 1, **wherein** said user identification code being also a predetermined number of said graphic symbols selectable from said displayed set of graphic symbols.

3. The authorisation method as claimed in claim 1, **wherein** in said displaying step showing to said user on said remote terminal respective lists associated with each of said features, each list comprising in a consecutive order all variations of the feature concerned, and allowing for said user to select from said lists in association with every generated symbol.

4. The authorisation method as claimed in claim 3, **wherein** respective features being the shape, the colour and a number written on each of said symbols.

5. The authorisation method as claimed in claim 1, **wherein** said symbol set generating algorithm comprises selection criteria of features.

6. The authorisation method as claimed in claim 1, **wherein** said symbol set generating algorithm comprises selection and modification criteria of said features.

7. The authorisation method as claimed in claim 1, further **comprising** the step of carrying out a transformation on said generated symbols to obtain a

longer sequence of characters, defined as cryptographic key, before being forwarded from said remote terminal to said authorisation centre, and in said authorisation centre using the same transformation, and in said comparing step comparing said transformed versions of the generated and reproduced symbols.

8. The authorisation method as claimed in claim 1, **wherein** in said communication between said remote terminal and said authorisation centre the transmittal of the identification code and the identification of the user at the authorisation centre preceding said displaying step, and in said displaying step constructing said table of graphic symbols in the knowledge of said symbol set generating algorithm associated with the particular user so that said algorithm becomes always applicable.

9. The authorisation method as claimed in claim 8, further **comprising** the step of carrying out a transformation on said generated symbols to obtain a longer sequence of characters, defined as cryptographic key, before being forwarded from said remote terminal to said authorisation centre, using said cryptographic key for encrypting a message from said user to the authorisation centre, and in said authorisation centre using the same transformation to obtain said cryptographic key, and using said key to decrypt the forwarded information, and in said comparing step decrypting the received information, and the comparison is regarded positive when the decrypted information fulfils certain conditions known to the remote terminal and to the authorisation centre.

10. The authorisation method as claimed in claim 9, further **comprising** the step of carrying out a transformation on said generated symbols to obtain a longer sequence of characters, defined as cryptographic key and carrying out a still another transformation on said generated symbols to obtain a unique cryptographic algorithm, before being forwarded from said remote terminal to said authorisation centre, using said cryptographic key and said unique cryptographic algorithm for encrypting a message from said user to the

authorisation centre, and in said authorisation centre using the same transformation to obtain said cryptographic key and said cryptographic algorithm, and using said key and said algorithm to decrypt the forwarded information, and in said comparing step decrypting the received information, and the comparison is regarded positive when the decrypted information fulfils certain conditions known to the remote terminal and to the authorisation centre.

11. The authorisation method as claimed in claim 10, further **comprising** the step of creating a digital fingerprint (message authentication code, MAC) from the message of the user with the help of a one way hash function, encrypting the digital fingerprint using the said cryptographic key and unique cryptographic algorithm, forwarding from said remote terminal to said authorisation centre the message and the encrypted digital fingerprint, in said authorisation centre creating a digital fingerprint (message authentication code, MAC) from the message received from the user and using the same transformation to obtain said cryptographic key and said cryptographic algorithm, and using said key and said algorithm to decrypt the digital fingerprint forwarded with the message and in said comparing step decrypting the received digital fingerprint and the comparison is regarded positive when the decrypted digital fingerprint and the digital fingerprint created in the authorisation centre are identical.